IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	Raikar et al	Patent Application	
Serial No.:	10/600,113	Group Art Unit:	2136
Filed:	June 20, 2003	Examiner:	David Cervetti

For: INTEGRATED INTRUSION DETECTION SYSTEM AND METHOD

Appeal Brief

Table of Contents

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Company.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-16 remain pending. Rejections of Claims 1-16 is herein appealed. Claims 17-20 are cancelled.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claim 1 recites an integrated intrusion detection method (method 200 of Figure 2 and page 15, lines 20-25). The method includes gathering (210 of Figure 2 and page 16, lines 1-19) information from a plurality of different types of intrusion detection sensors, processing (220 of Figure 2 and page 16, lines 20-26 through page 20, line 14) the information, wherein the processing provides a consolidated correlation of the information, assigning a severity to the information based on an enterprise wide security policy. The method also includes assigning (230 of Figure 2 and page 20, lines 14-26) a response corresponding to the information and corresponding to the severity; and implementing (240 of Figure 2 and page 21, lines 4-26) the response according to the severity.

Independent Claim 8 recites a computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement intrusion detection instructions. The computer usable storage medium comprising a data collection module (102 of Figure 1 and page 9, line 3) for receiving information from a plurality of different types of intrusion detection sensors, wherein the information indicates potential security issues, an information severity determination module for assigning a severity to said information based on an enterprise wide security policy, an integration module (104 of Figure 1 and page 9, line 26) for integrating the information in a network application management platform, a reaction determination module (105 of Figure 1 and page 10, line 25) for determining appropriate response to indication of the potential security issues according to the severity and a reaction direction module (107 of Figure 1 and page 10, line 25) for directing the response according to the severity.

Grounds of Rejection to be Reviewed on Appeal

1. **Claims 1-17 stand rejected under 35 U.S.C. 102(a) as being anticipated by Schneier (2002/0087882).**

Arguments

1. **Whether Claims 1-17 are anticipated by Schneier (2002/0087882).**

35 U.S.C. §102(a) – Claims 1-17

Claims 1-17 are rejected under 35 U.S.C. 102(a) as being anticipated by Schneier (2002/0087882). The rejection is respectfully traversed for the following rational.

Applicants have amended Independent Claims 1 and 8 to include the feature "assigning a severity to said information based on an enterprise wide security policy." Support for the newly added features of Independent Claims 1 and 8 can be found at least on page 18, lines 18-23.

Applicants do not understand Schneier to anticipate this claimed feature.

MPEP §2131 provides:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). … "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

Applicants respectfully submit that Schneier fails to anticipate this claimed feature.

For this rational, Applicants submit that Independent Claims 1 and 8 and subsequently dependent Claims 2-7 and 9-16 are patentable over Schneier and Applicants respectfully request the rejection be removed.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellant's undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNER BLECHER LLP

Date: 11/17/2008

/John P. Wagner, Jr./

John P. Wagner, Jr.

Registration Number: 35,398

WAGNER BLECHER LLP
WESTRIDGE BUSINESS PARK
123 WESTRIDGE DRIVE
WATSONVILLE, CALIFORNIA 95076
408-377-0500

Claims Appendix

1. An integrated intrusion detection method comprising:

gathering information from a plurality of different types of intrusion detection sensors;

processing said information, wherein said processing provides a consolidated correlation of said information;

assigning a severity to said information based on an enterprise wide security policy;

assigning a response corresponding to said information and corresponding to said severity; and

implementing said response according to said severity.

2. An integrated intrusion detection method of Claim 1 wherein said information includes intrusion detection alerts.

3. An integrated intrusion detection method of Claim 2 further comprising centrally tracking information associated with intrusion detection alerts from said plurality of different types of intrusion detection sensors.

4. An integrated intrusion detection method of Claim 3 wherein said tracking information associated with intrusion detection includes assigning severity assignments standardized across said plurality of different types of intrusion detection sensors.

5. An integrated intrusion detection method of Claim 2 wherein said intrusion detection alerts are correlated based upon various alert attributes.

6. An integrated intrusion detection method of Claim 2 wherein said response conforms to an enterprise wide strategy.

7. An integrated intrusion detection method of Claim 1 further comprising managing said intrusion detection sensors.

8. A computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement intrusion detection instructions comprising:

a data collection module for receiving information from a plurality of different types of intrusion detection sensors, wherein said information indicates potential security issues;

an information severity determination module for assigning a severity to said information based on an enterprise wide security policy;

an integration module for integrating said information in a network application management platform;

a reaction determination module for determining appropriate response to indication of said potential security issues according to said severity; and

a reaction direction module for directing said response according to said severity.

9. A computer usable storage medium of Claim 8 wherein said information includes intrusion detection system alert data.

10. A computer usable storage medium of Claim 8 wherein said integration module selects a hook in an intrusion detection system.

11. A computer usable storage medium of Claim 8 wherein said data collection module logs alerts from said plurality of different types of intrusion detection sensors.

12. A computer usable storage medium of Claim 8 wherein said alerts are provided by a simple network management protocol (SNMP), a system log and an application program interface.

13. A computer usable storage medium of Claim 8 wherein said integration module includes analyzing a plurality of manners in which an alert can be provided and selecting the manner that is the most secure with the least dependencies in a communication path.

14. A computer usable storage medium of Claim 8 wherein said integration module utilizes a network application management platform to log information.

15. A computer usable storage medium of Claim 14 wherein:

an open view operation simple network management protocol trap is utilized to handle simple network management protocol trap based alerts;

an open view operation log file encapsulator handles system log based alerts; and

an open view message interceptor handles application program interface propagated alerts with the help of an operation message mechanism.

16. A computer usable medium of Claim 14 wherein a secure open view template configuration is utilized to log information and the one message group is configured for handling intrusion detection system alerts and another message group is configured for handling intrusion detection system errors.

Evidence Appendix

None

Related Proceedings Appendix

None